#2

FORM PTO-1449 (Modified) LIST OF PATENTS AND PUBLICATIONS FOR APPLICANT'S INFORMATION DISCLOSURE STATEMENT (Use several sheets if necessary)	ATTY. DOCKET NO. RSW920000091US1	SERIAL NO. Not Yet Assigned
	APPLICANT: Gennaro, Rosario	
	FILING DATE: Herewith	GROUP: To be assigned

jc843 U.S. PTO 09/753727 01/03/01

REFERENCE DESIGNATION **U.S. PATENT DOCUMENTS**

EXAMINER INITIALS		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE (IF APPRO.)
MTH	AA	5 9 0 9 4 9 4	Jun. 1, 1999	Blaze	380	37	Feb. 14, 1997
MTH	AB	5 7 8 4 0 0 2	Jul. 21, 1998	Roehr	340	825.5	May 2, 1995
MTH	AC	4 5 1 1 9 8 8	Apr. 16, 1985	Michel et al.	364	717	Jul. 16, 1982
MTH	AD	4 9 4 4 0 0 9	Jul. 24, 1990	Micali et al.	380	46	Feb. 25, 1988
MTH	AE	4 3 6 9 5 1 2	Jan. 18, 1983	Brossard et al.	371	43	Oct. 23, 1980
MTH	AF	3 7 2 8 6 7 8	Apr. 17, 1973	Tong	340	146.1	Sept. 3, 1971

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	TRANSLATION YES	TRANSLATION NO
MTH	AG	0 1 7 4 0 2 8	March 12, 1986	European	H 03 M	7/24		

OTHER ART (Including Author, Title, Date, Pertinent Pages, etc.)

MTH	AH		1998 Society for Industrial and Applied Mathematics, Siam J. Comput, "The Discrete Logarithm Hides 0(log n) Bits", Long and Wigderson, Vol. 17, No. 2, April 1998, pp. 363-372

#2

MTH	AI		Computer Science Division University of California, Berkley, California, Rene Peralla "Simultaneous Security of Bits in the Discrete Log", pp.62-72
MTH	AJ		1996 Society for Industrial Mathematics, Siam J. Comput, "A Simple Unpredictable Pseudo-Random Number Generator", L. Blum, M. Blum and M Shubs. Vol. 15, No. 2, May 198, pp. 364-383.
MTH	AK		Bit Security of RSA and Rabin Functions, "RSA and Rabin Functions Certain Parts are as Hard as the Whole", W. Alex, B. Chor O. Goldreich and C. Schnorr, Vol. 1, No. 2, April 1988, pp. 194-209
MTH	AL		Bell Labs, "An Efficient Discrete Log Pseudo Random Generator", S. Patel and G. Sundaram, pp. 304-317
MTH	AM		Siam J. Comput, "How to Generate Cyrptographically Strong Sequences of Pseudo-Random Bits", M. Blum and S. Mical, Vol. 13, No. 4, Nov. 1984, pp. 850-864
MTH	AN		Journal of Computer and System Sciences 18, 143-154 (1979), "Universal Classes of Hash Functions", J. Lawrence Carter and M. N. Wegman, received August 8, 1977, revised August 10, 1978
MTH	AO		Mihir Bellare (Ed.), "Advances in Cryptology CRYPTO 2000", 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000 Proceedings

EXAMINER	DATE CONSIDERED
	7/23/04

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.